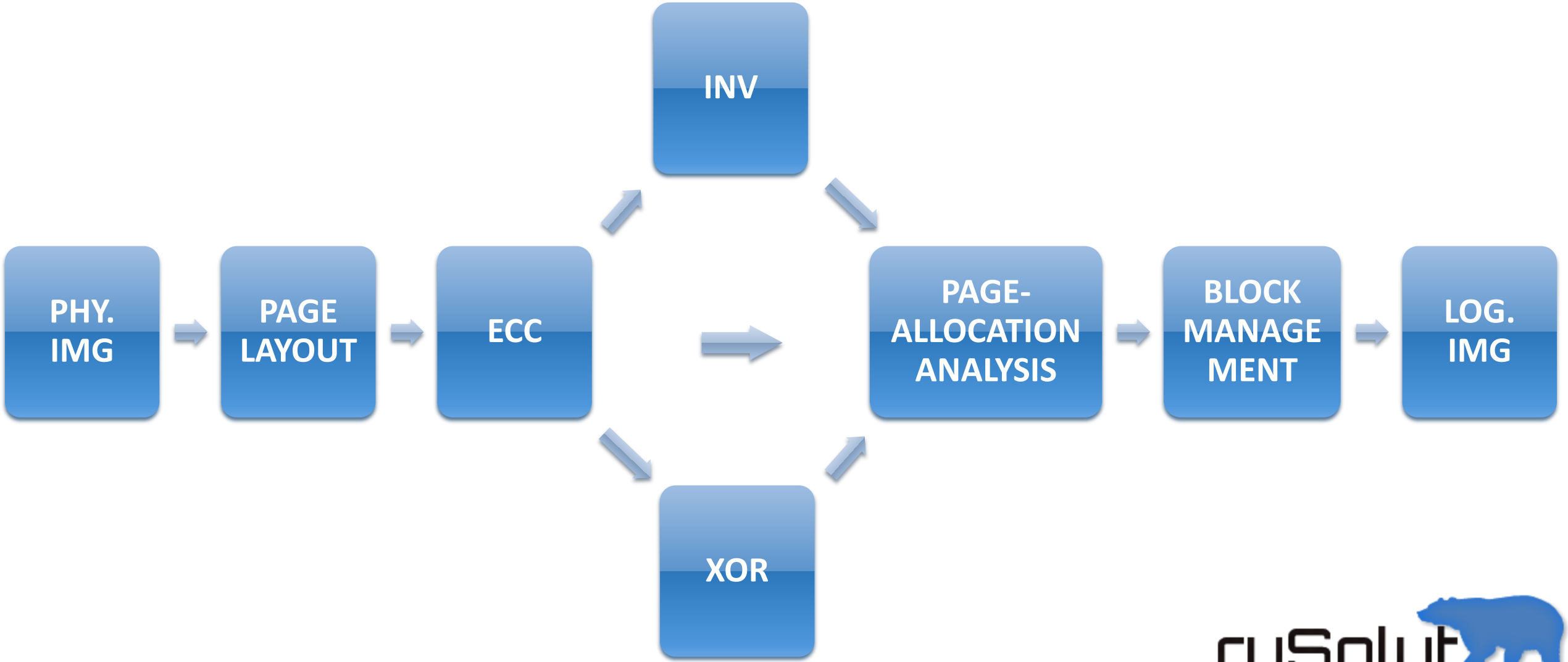
Block management.
LBN, headers, Marker table.

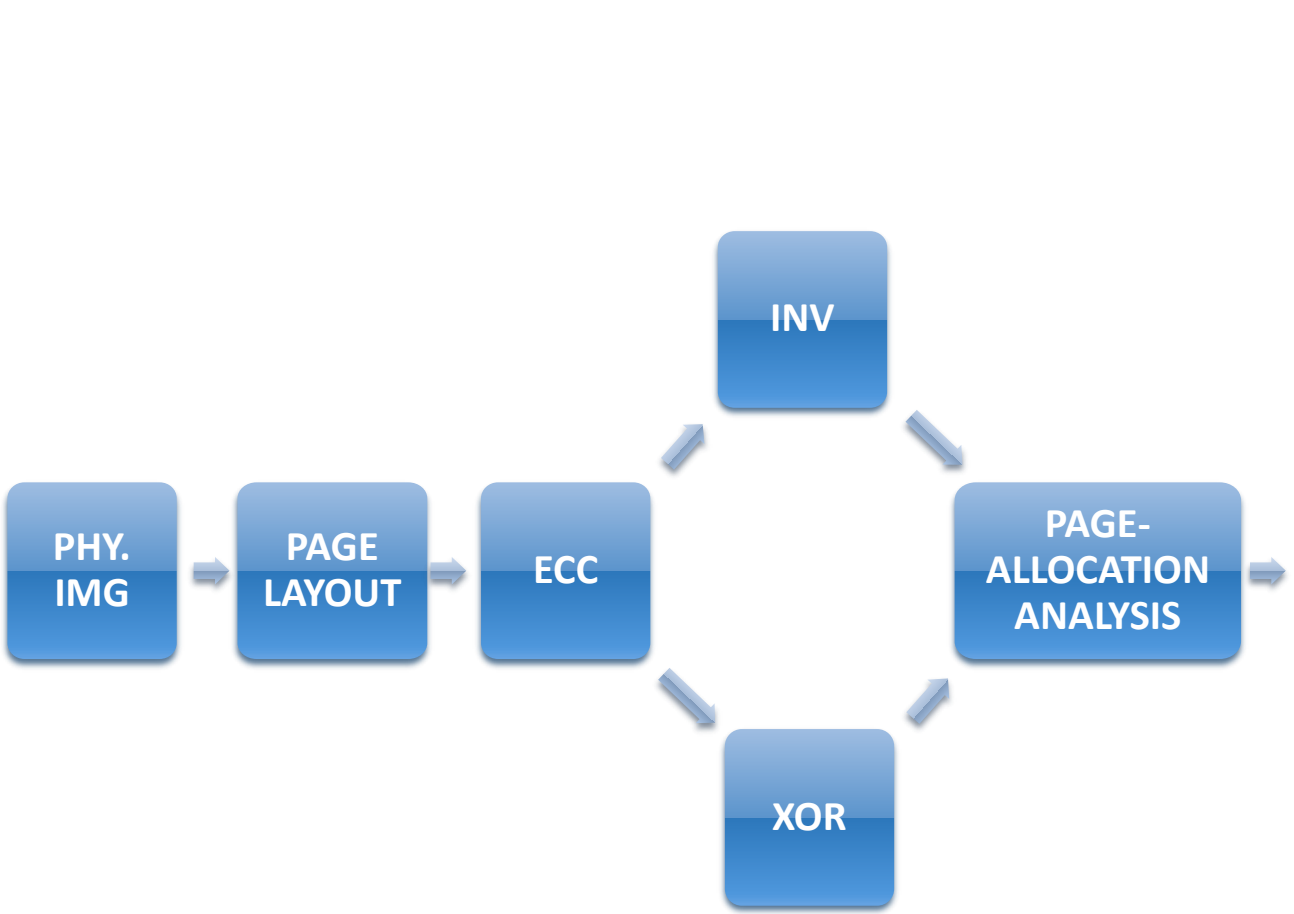
Igor Loskutov, Rusolut

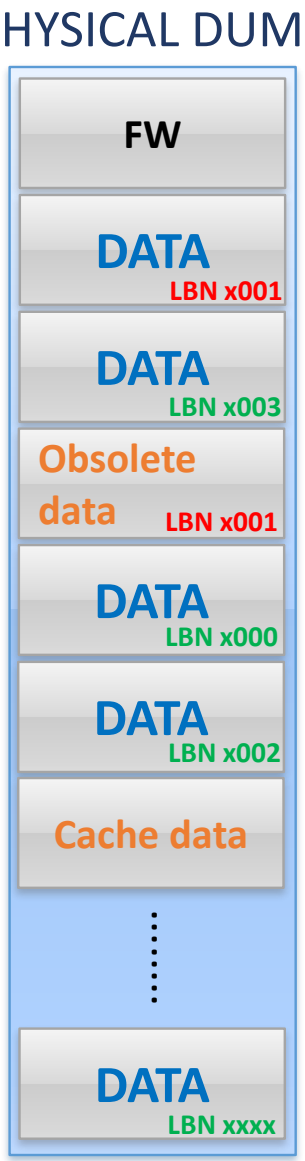
PHYSICAL TO LOGICAL DUMP TRASFORMATION
(reverse operations)



ruSolut
Data Investigation & Recovery Technology

BLOCK MANAGEMENT

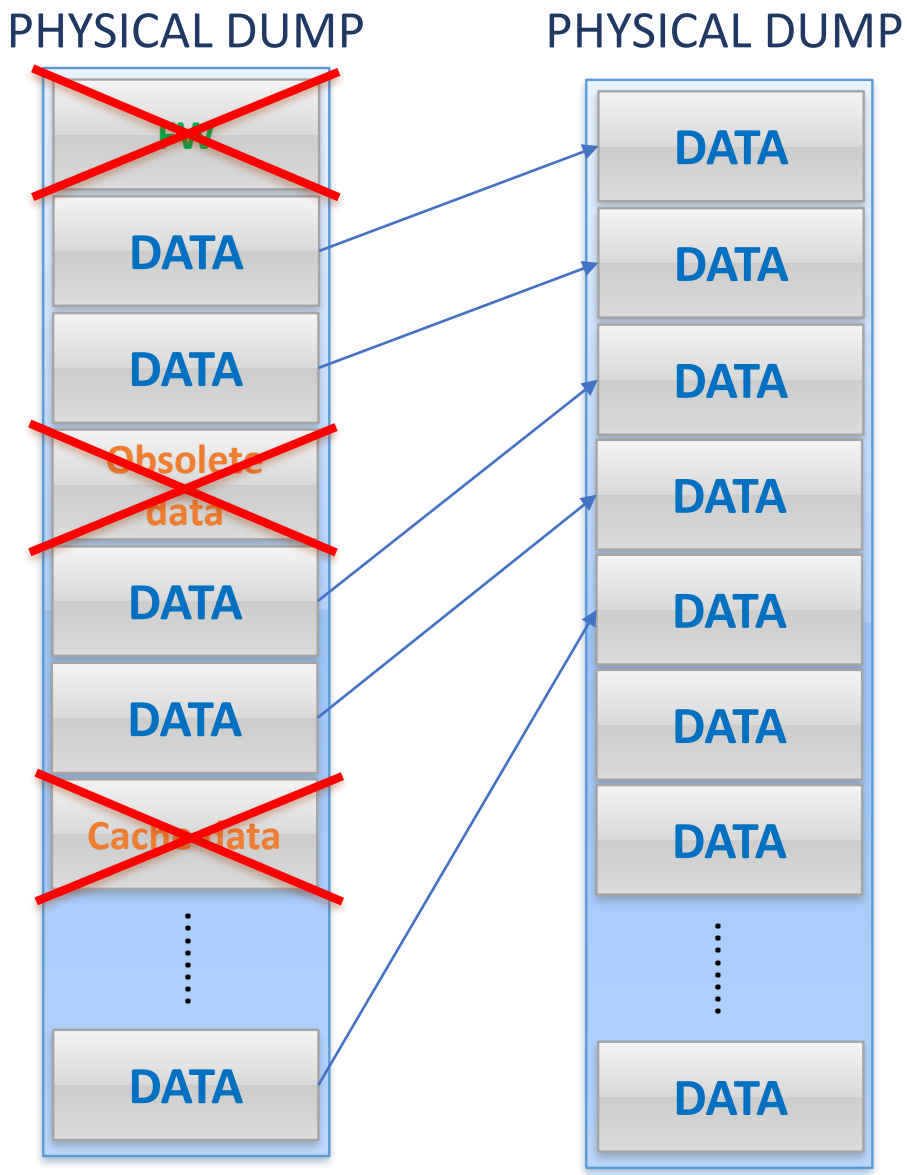




The physical dump contains blocks with actual user data, obsolete user data, cache blocks, and firmware/system blocks.

ruSolut
Data Investigation & Recovery Technology

BLOCK MANAGEMENT

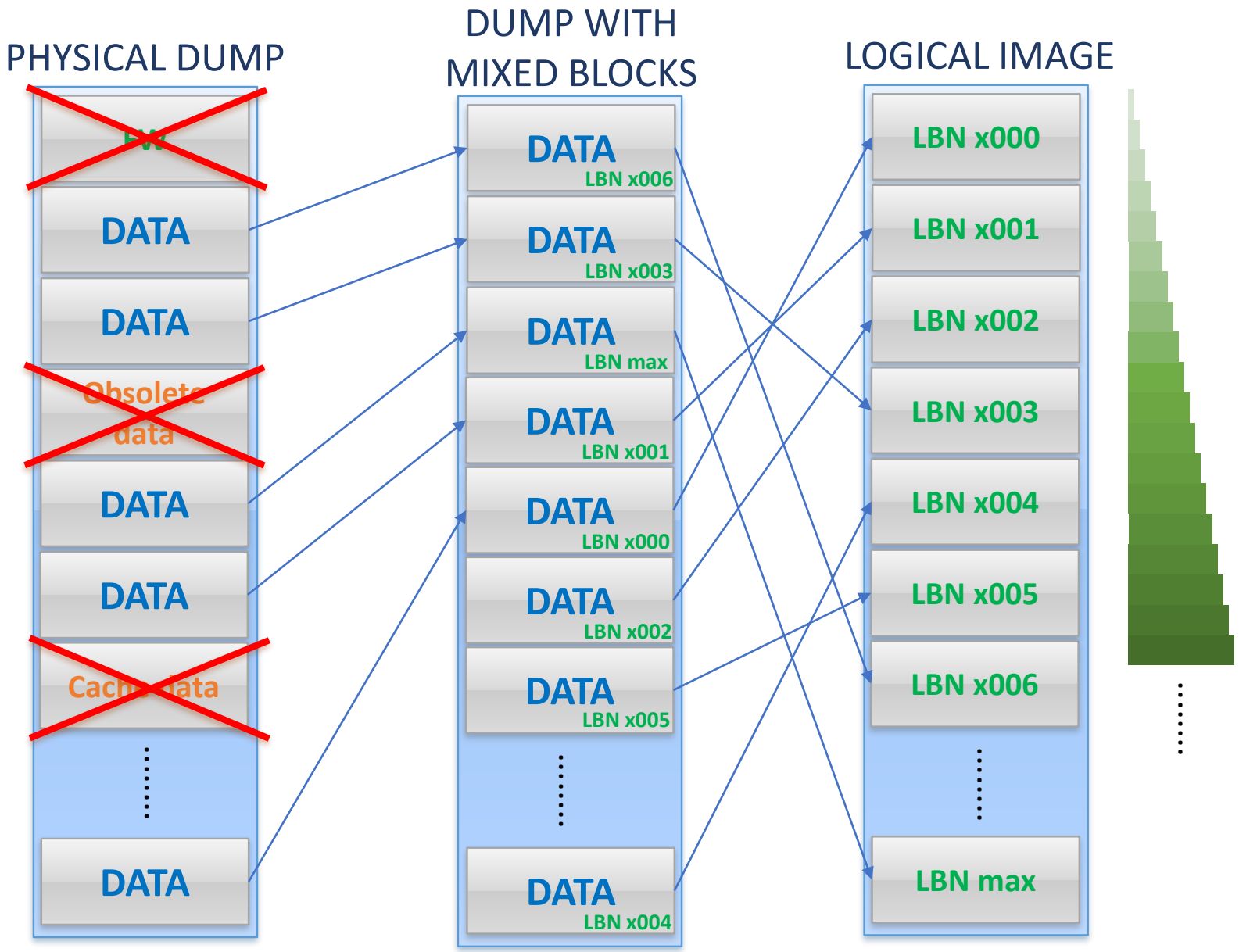


The **BLOCK MANAGEMENT** stage is where:

1. blocks WITHOUT user data are filtered out and removed by their **HEADER**.

ruSolut
Data Investigation & Recovery Technology

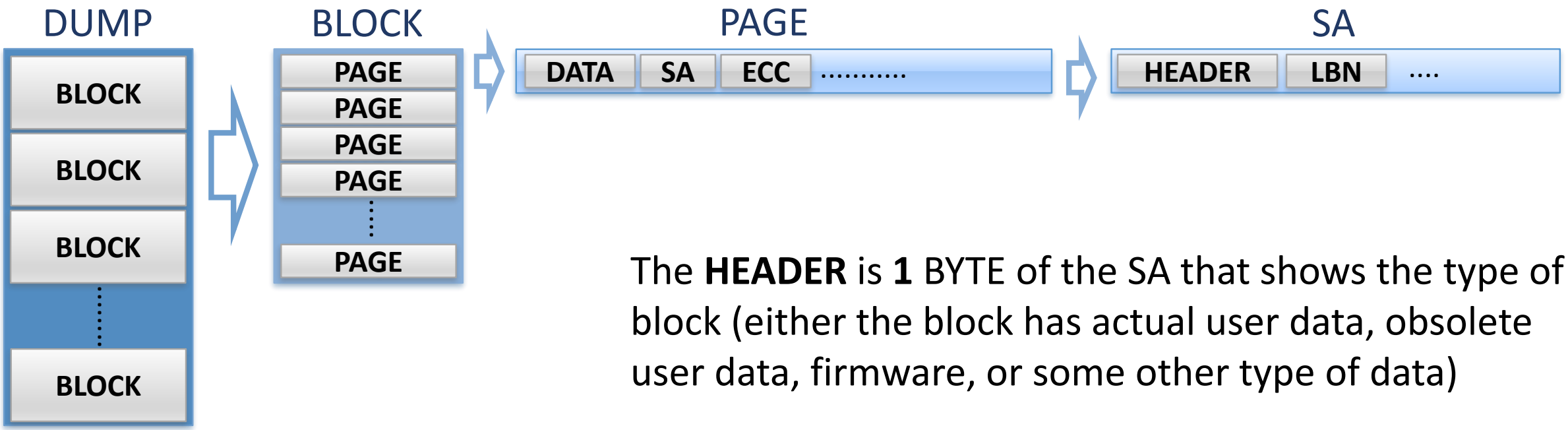
BLOCK MANAGEMENT



2. blocks WITH user data are arranged in ascending order by **LBN**.

ruSolut
Data Investigation & Recovery Technology

BLOCK MANAGEMENT



The **HEADER** is **1** BYTE of the SA that shows the type of block (either the block has actual user data, obsolete user data, firmware, or some other type of data)

The **LBN** (logical block number) is **2** BYTES of the SA that defines the number (position) of the block in the logical image.

ruSolut
Data Investigation & Recovery Technology

HEADER

The **HEADER** is **1** BYTE of the SA that shows the type of block (either the block has actual user data, obsolete user data, firmware, or some other type of data)

The header of user data blocks may have:	one specific value (FF, 00, and so on)
	several specific values (FF/50, FF/00, and so on)
	a range of values (20-3F, 21-3F, and so on)

Normally, the majority of the blocks in the physical dump have actual user data, so the majority of the blocks should have the same HEADER

To filter out blocks without actual user data, it is necessary to:

Find the header that the majority of the blocks with data have → Filter out and remove blocks with a different header

LBN

The **LBN** (logical block number) is **2** BYTES of the SA that defines the number (position) of the block in the logical image.

Typical LBN ranges:	0000-03FF; 0000-07FF; 0000-0FFF
	1000-13FF; 1000-17FF; 1000-1FFF
	x000-x3FF; x000-x7FF; x000-xFFF

The LBN may be:

INVERTED	RECORDED IN LITTLE-ENDIAN ORDER
• FFFF- 0C00 (numbers are too large and there are no LBN values close to 0000)	• 0000 • 0001 • 0100 • 0101 • … • FF00 • FF01

ruSolut
Data Investigation & Recovery Technology

LBN

INVERTED

Use	Bank	LBN	Header	Address	LB	RB
☑	00	F886	21	01D87D0000	☐	☐
☑	00	F887	21	01D8C20000	☐	☐
☑	00	F888	21	01D9070000	☐	☐
☑	00	F889	21	01D94C0000	☐	☐
☑	00	F88A	21	003D2F0000	☐	☐
☑	00	F88B	21	01AB350000	☐	☐
☑	00	F88C	21	01D9910000	☐	☐
☑	00	F88D	22	0215F10000	☐	☐
☑	00	F88E	21	01DA1B0000	☐	☐
☑	00	F88F	21	01DA600000	☐	☐
☑	00	F890	21	01DAA50000	☐	☐
☑	00	F891	21	01DAEA0000	☐	☐
☑	00	F892	21	01DB2F0000	☐	☐
☑	00	F893	21	01DB740000	☐	☐
☑	00	F894	21	01F5DE0000	☐	☐
☑	00	F895	21	01DBB90000	☐	☐
☑	00	F896	21	01DBFE0000	☐	☐
☑	00	F897	22	005F250000	☐	☐
☑	00	F898	23	00DF2C0000	☐	☐
☑	00	F899	22	01DD9C0000	☐	☐
☑	00	F89A	22	01DE260000	☐	☐
☑	00	F89B	22	006C150000	☐	☐
☑	00	F89C	22	01DE6B0000	☐	☐
☑	00	F89D	22	01DEF50000	☐	☐
☑	00	F89E	22	01DF3A0000	☐	☐
☑	00	F89F	22	01DF7F0000	☐	☐
☑	00	F8A0	22	01DFC40000	☐	☐
☑	00	F8A1	22	01E0090000	☐	☐

•FFFF- 0C00 (numbers are too large and there are no LBN values close to x000)

RECORDED IN LITTLE-ENDIAN ORDER

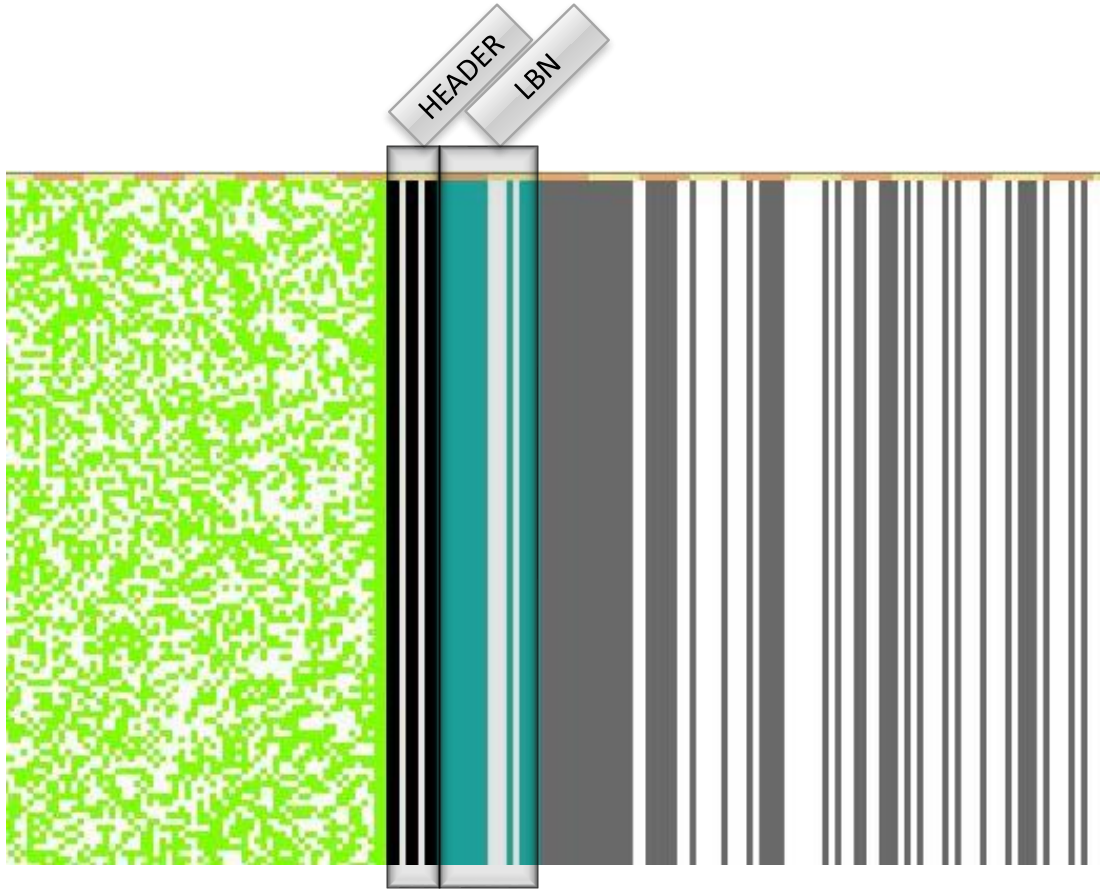
Use	Bank	LBN	Header	Address	LB	RB
☑	00	0000	44	0004C0E000	☐	☐
☑	00	0001	11	0003246000	☐	☐
☑	00	0002	11	0007B7E000	☐	☐
☑	00	0003	11	000BCFA000	☐	☐
☑	00	0100	11	0001188000	☐	☐
☑	00	0100	44	000124E000	☐	☐
☑	00	0101	11	000665A000	☐	☐
☑	00	0102	11	0007BC0000	☐	☐
☑	00	0103	11	000BD3C000	☐	☐
☑	00	0200	11	0001C9E000	☐	☐
☑	00	0201	11	000F468000	☐	☐
☑	00	0202	11	0006C8A000	☐	☐
☑	00	0203	11	000BD7E000	☐	☐
☑	00	0300	11	0001CE0000	☐	☐
☑	00	0301	11	000376E000	☐	☐
☑	00	0302	11	0006CCC000	☐	☐
☑	00	0303	11	000BDC0000	☐	☐
☑	00	0400	11	0001D22000	☐	☐
☑	00	0401	11	0003414000	☐	☐
☑	00	0402	11	0007C02000	☐	☐
☑	00	0403	11	000BE02000	☐	☐
☑	00	0500	11	0001D64000	☐	☐
☑	00	0501	11	0005490000	☐	☐
☑	00	0502	11	0007C44000	☐	☐
☑	00	0503	11	000BE44000	☐	☐
☑	00	0600	11	0001DA6000	☐	☐
☑	00	0601	11	00032CA000	☐	☐
☑	00	0602	11	0007C86000	☐	☐
☑	00	0603	11	000BE86000	☐	☐

•High-order byte continuously grows, Low-order byte repeats several values (00,01,02,03,00,01,02,03,00,01,02,03….)

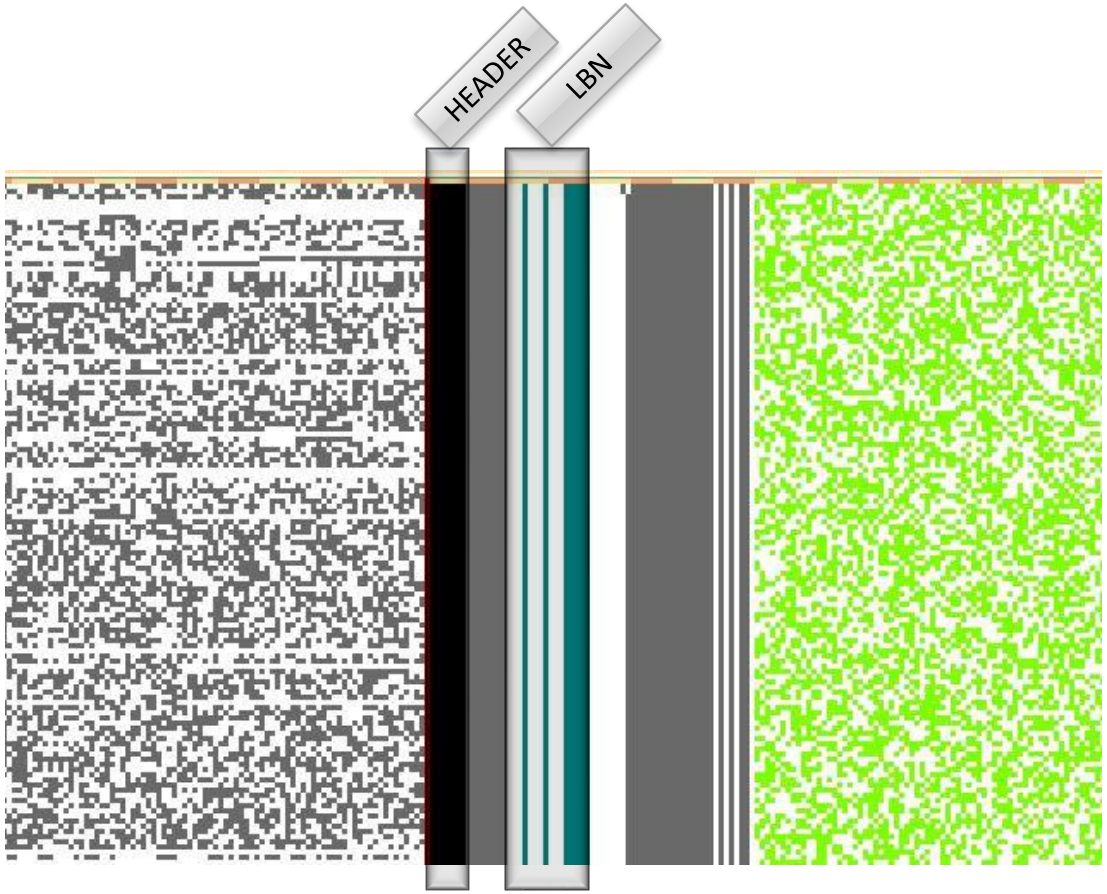
ruSolut
Data Investigation & Recovery Technology

HEADER AND LBN TYPICAL LOCATIONS IN THE SA

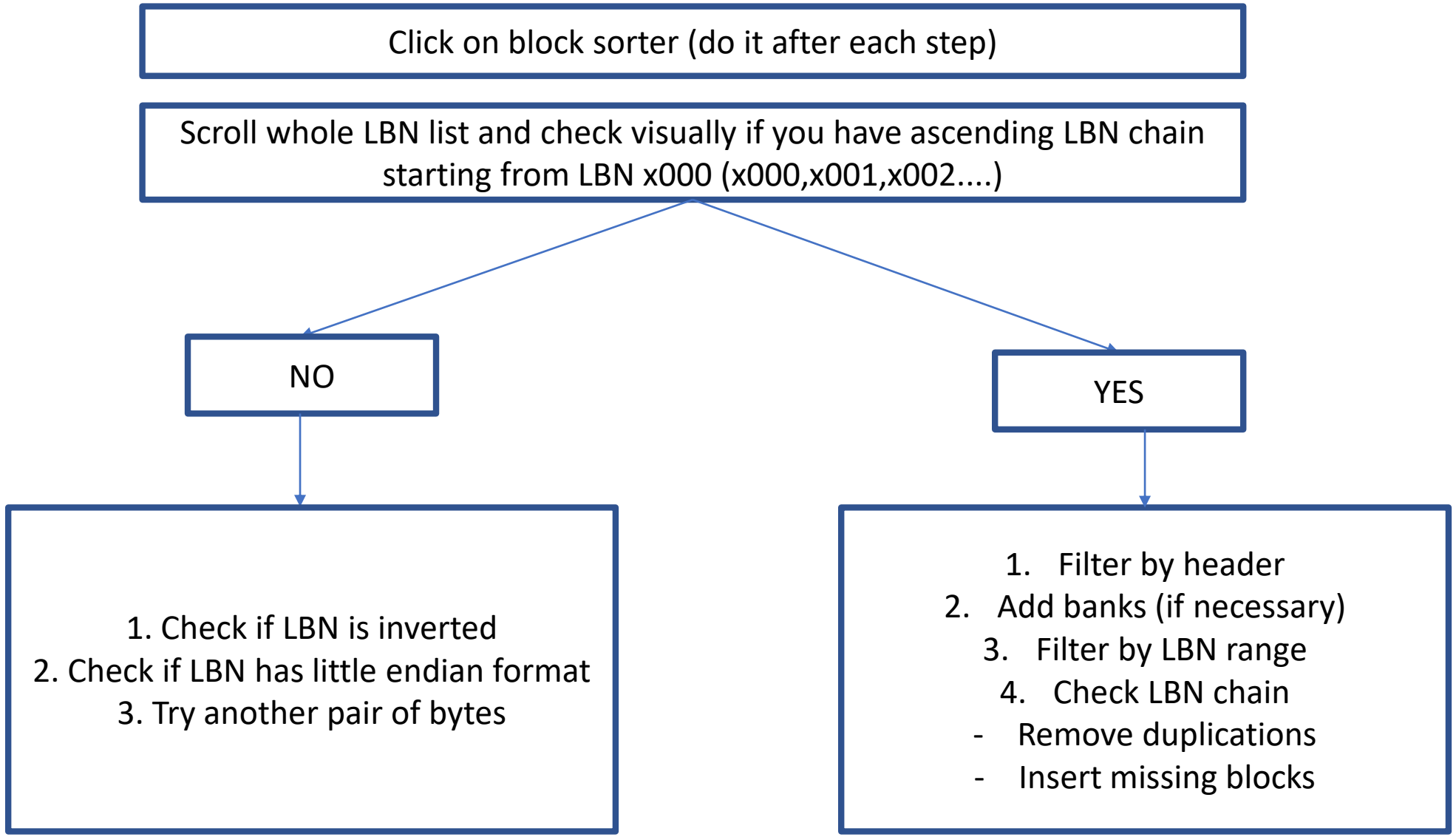
SM controllers



PHISON controllers

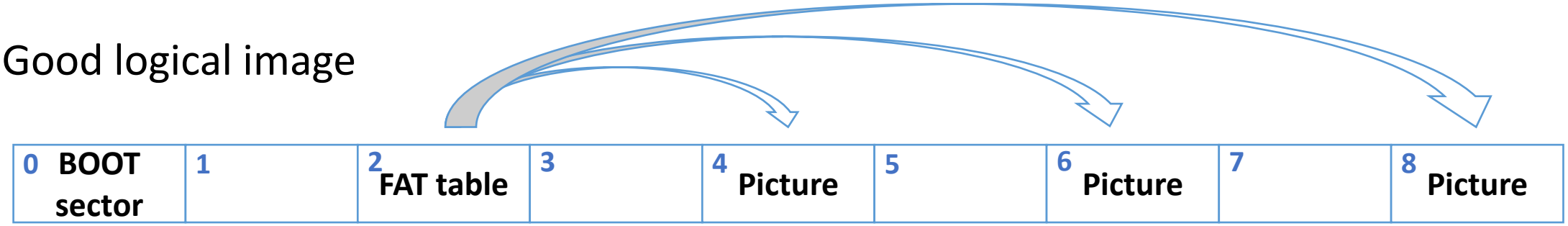


BLOCK MANAGEMENT

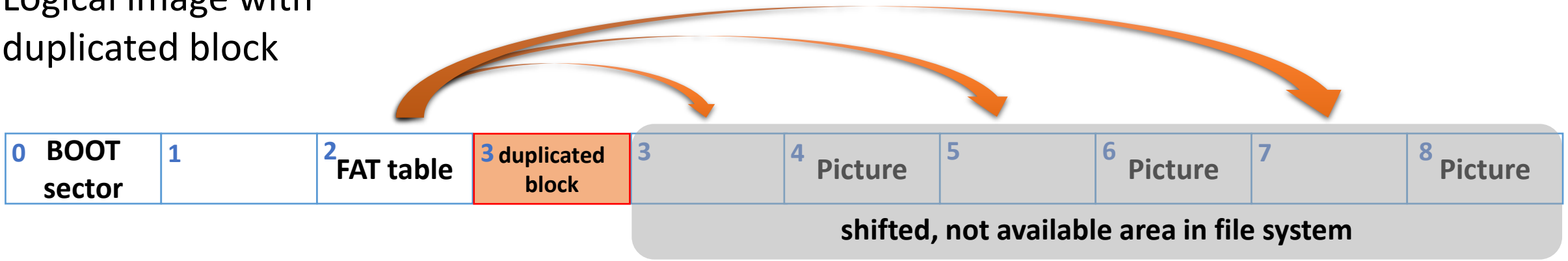

Click on block sorter (do it after each step)
Scroll whole LBN list and check visually if you have ascending LBN chain starting from LBN x000 (x000,x001,x002....)
NO
YES
1. Check if LBN is inverted
2. Check if LBN has little endian format
3. Try another pair of bytes
1. Filter by header
2. Add banks (if necessary)
3. Filter by LBN range
4. Check LBN chain
- Remove duplications
- Insert missing blocks

DUPLICATED BLOCKS

Good logical image

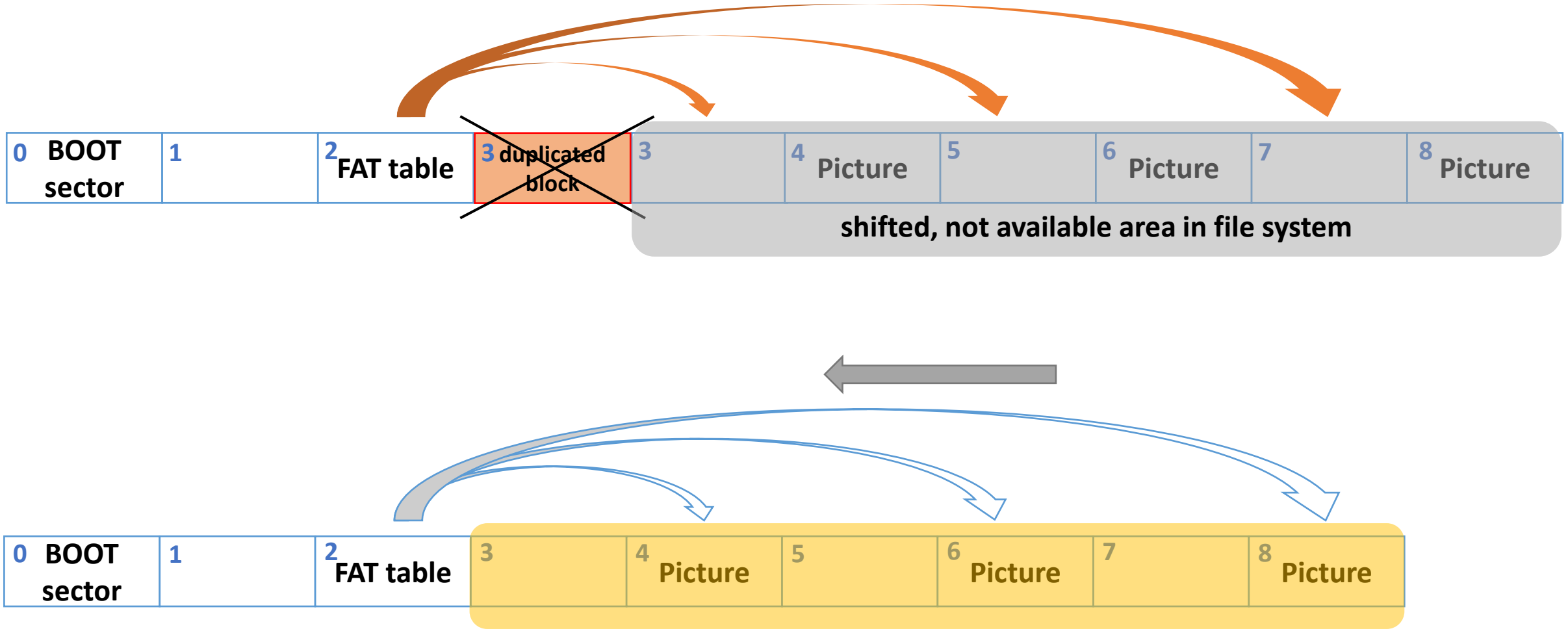


Logical image with duplicated block



ruSolut
Data Investigation & Recovery Technology

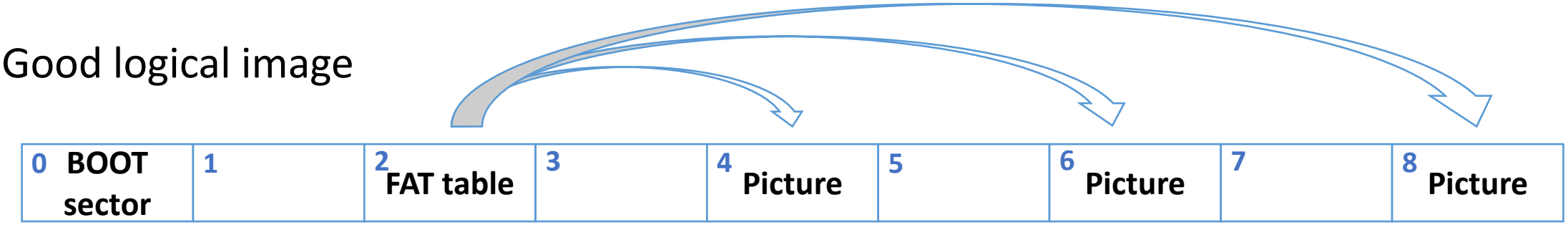
DUPLICATED BLOCKS



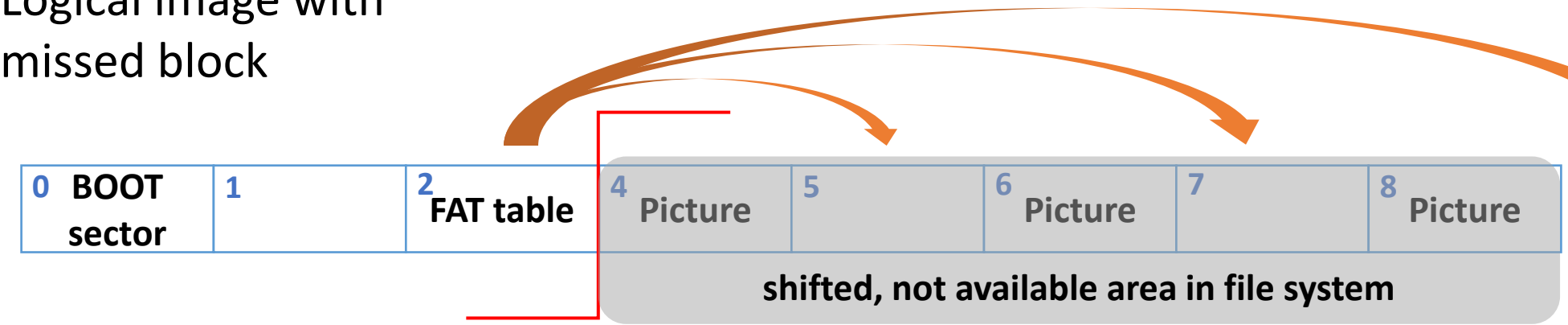
ruSolut
Data Investigation & Recovery Technology

MISSING BLOCKS

Good logical image

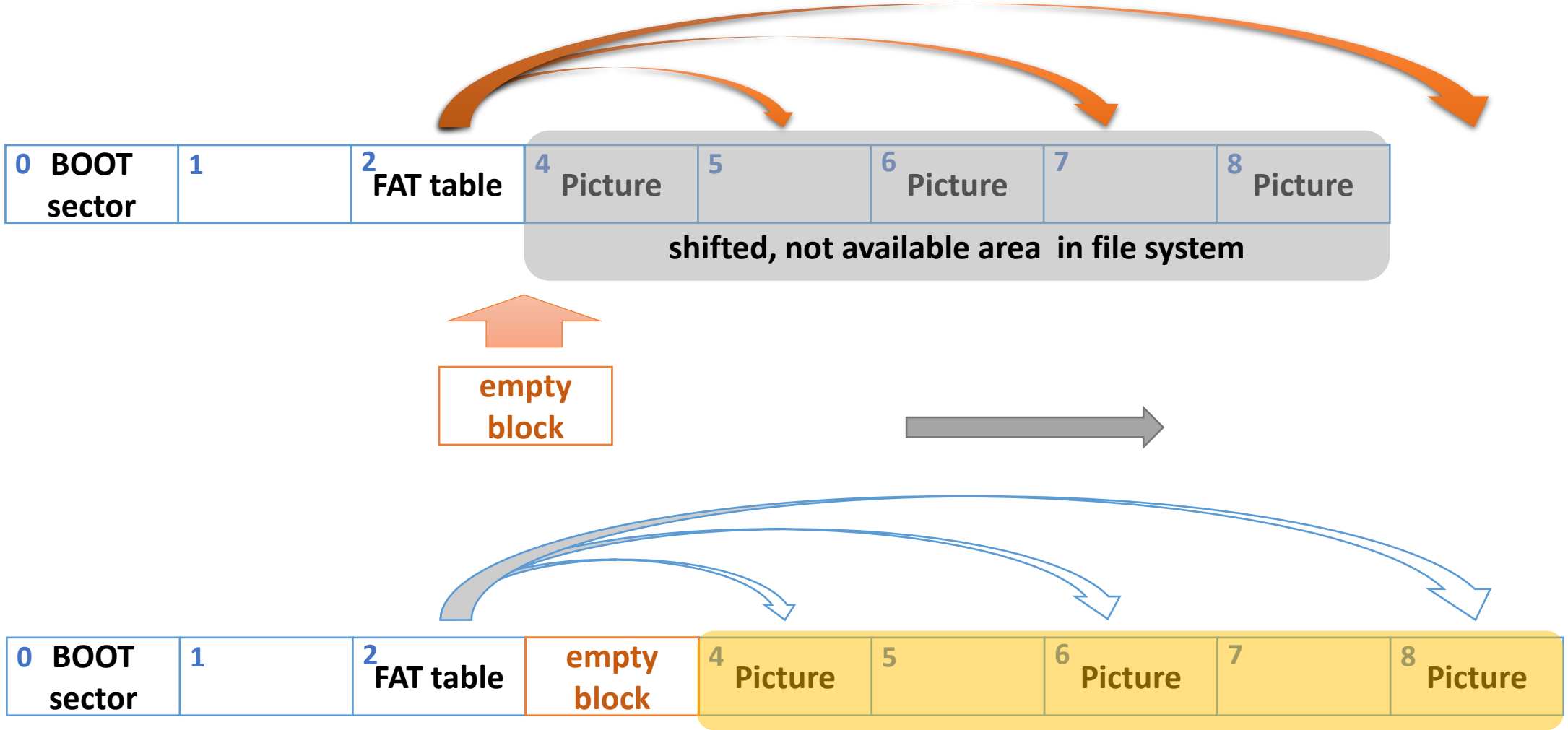


Logical image with missed block



ruSolut
Data Investigation & Recovery Technology

MISSING BLOCKS



ruSolut
Data Investigation & Recovery Technology

LBN CHAIN TEST STEP

Step syntaxis

x/y	x- High-order byte increment step y- Low-order byte increment step

Examples

1/1

0000
0001
0002
⋮
00FF
0100
0101
⋮
01FF
0200
0201

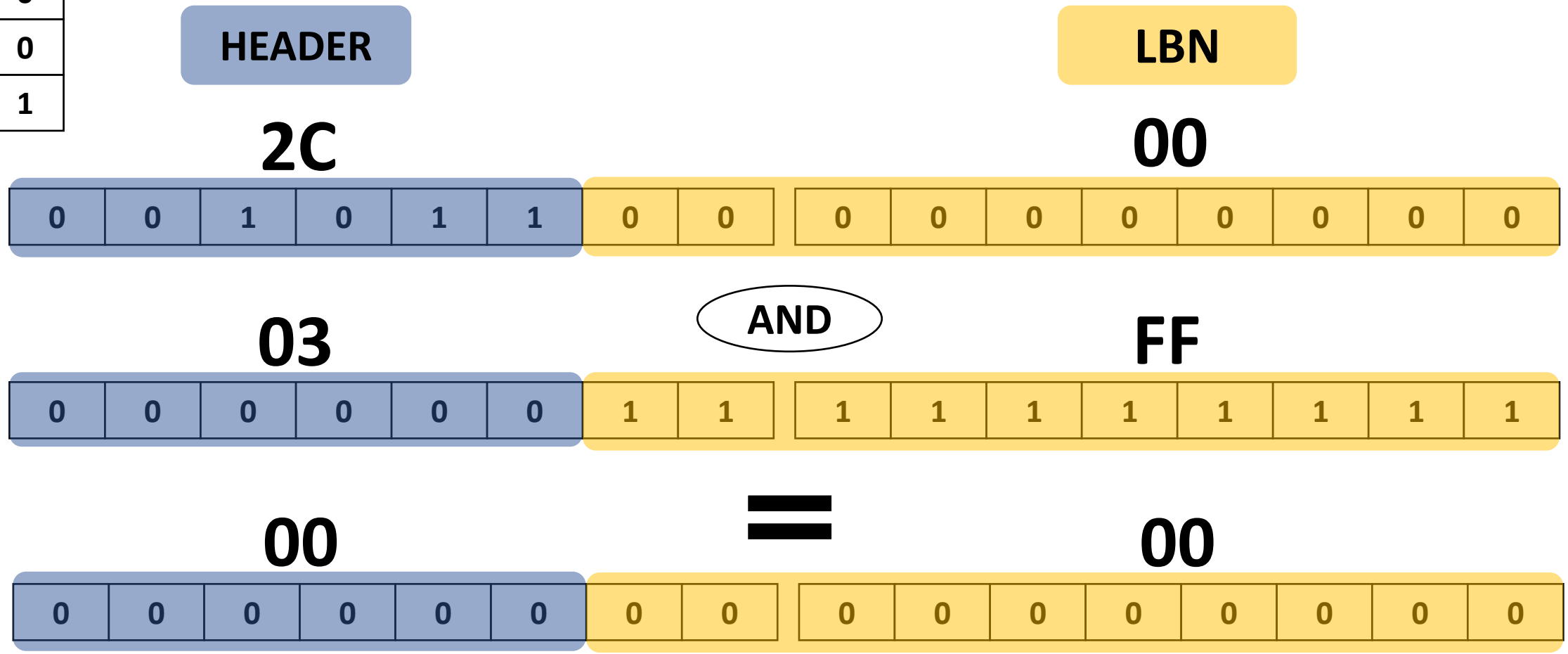
10/1

8000
8001
8002
⋮
80FF
9000
9001
⋮
90FF
A000
A001

ruSolut
Data Investigation & Recovery Technology

MASK

A	B	AND
0	0	0
0	1	0
1	0	0
1	1	1



ruSolut
Data Investigation & Recovery Technology